Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method comprising:

collecting information associated with a group of users visiting a web site;

identifying [[real]] non-malicious users visiting [[a]] the web site from the group of users visiting the web site based on the collected information; and

determining an occurrence of spamming on the web site based at least in part on ~~the identified real users~~ a behavior of the identified non-malicious users.

2. (currently amended) The method of claim 1 wherein the ~~identifying real users~~ collecting information includes:

tracking activities of the group of users visiting the web site~~, and~~

~~identifying the real users based at least in part on the tracked activities~~.

3. (currently amended) The method of claim 2 wherein the tracking activities includes:

determining whether the users in the group of users load images.

4. (currently amended) The method of claim 2 wherein the tracking activities includes:

determining whether the users in the group of users have javascript turned on.

5. (currently amended) The method of claim 2 wherein the tracking activities includes:

determining a type of browser used by the users in the group of users.

6. (currently amended) The method of claim 2 wherein the tracking activities includes:

determining an interval at which each of the users in the group of users visits the web site.

7. (currently amended) The method of claim 2 wherein the web site is a search engine, and

wherein the tracking activities includes:

determining a type of items for which searches are performed by the users in the group of users.

8. (currently amended) The method of claim 2 wherein the tracking activities includes:

tracking activities of users in the group of users visiting another web site.

9. (currently amended) The method of claim 2 wherein each of the users in the group of users is associated with a cookie identifier, and

wherein the tracking includes:

using the cookie identifiers to track the activities of the users in the group of users.

10. (currently amended) The method of claim 1 wherein each of the users in the group of users is associated with a cookie identifier, and

wherein the identifying [[real]] non-malicious users includes:

identifying [[real]] non-malicious users based at least in part on an age of the cookie identifiers associated with the users in the group of users.

11. (currently amended) The method of claim 1 wherein each of the users in the group of users is associated with a network address, and

wherein the identifying [[real]] non-malicious users includes:

identifying the [[real]] non-malicious users based at least in part on the network addresses associated with the users in the group of users.

12. (currently amended) The method of claim 1 wherein the web site includes at least one advertisement, and

wherein the determining an occurrence of spamming includes:

determining a click rate of the at least one advertisement for the identified [[real]] non-malicious users, and

determining that the at least one advertisement has been spammed when [[the]] a click rate of users in the group of users visiting the web site exceeds the determined click rate for the identified [[real]] non-malicious users.

13. (original) The method of claim 12 wherein the click rate includes a range of click rates.

14. (currently amended) The method of claim 1 wherein the web site includes at least one advertisement,

wherein the identifying includes:

determining a percentage of ~~a number of~~ users in the group of users visiting the web site in a time period that are [[real]] non-malicious users, and

wherein determining an occurrence of spamming includes:

estimating a percentage of [[real]] non-malicious users selecting the at least one advertisement during the time period to be approximately the percentage of [[real]] non-malicious users visiting the web site during the time period, and

determining that the at least one advertisement has been spammed when an actual percentage of [[real]] non-malicious users selecting the at least one advertisement during the time period is lower than the estimated percentage of [[real]] non-malicious users selecting the at least one advertisement during the time period.

15. (original) The method of claim 1 wherein the determining includes:

determining an occurrence of spamming of at least one advertisement on the web site, and

wherein the method further comprises:

providing a refund in response to determining that the at least one advertisement has been spammed.

16. (currently amended) A system comprising:

means for identifying ~~real users visiting~~ non-malicious visitors to a web site;

means for tracking at least one activity of the identified non-malicious visitors; and

means for determining an occurrence of click spamming on the web site based at least in part on ~~a behavior~~ the tracked at least one activity of the identified ~~real users visiting the web site~~ non-malicious visitors.

17. (currently amended) A computer-readable memory device containing instructions for controlling at least one processor to perform a method for detecting click spamming of an advertisement on a server, the method comprising:

determining a number of [[real]] non-malicious users accessing the server;

determining a percentage of the [[real]] non-malicious users clicking the advertisement when the advertisement is ~~displayed~~ provided to the [[real]] non-malicious users; and

determining whether the advertisement has been click spammed based at least in part on the determined percentage.

18. (currently amended) A server comprising:

a memory configured to store at least one advertisement; and

a processor configured to:

cause the at least one advertisement to be presented,

determine a number of [[real]] non-malicious users accessing the server,

determine a percentage of the [[real]] non-malicious users clicking the at least one advertisement, and

determine whether the at least one advertisement has been click spammed based at least in part on the determined percentage.

19. (currently amended) A method comprising:

identifying a group of [[real]] non-malicious users visiting [[the]] a web site;

determining a click rate of [[the]] an item associated with the web site for the group of [[real]] non-malicious users; and

determining whether the item has been click spammed based at least in part on the determined click rate for the [[real]] non-malicious users.

20. (currently amended) The method of claim 19 further comprising:

determining a total number of users visiting the web site, and

wherein the determining whether the item has been click spammed includes:

comparing the determined click rate for the [[real]] non-malicious users to a click rate for the total number of users visiting the web site, and

determining that the item has been click spammed when the click rate for the total number of users exceeds the determined click rate for the [[real]] non-malicious users.

21. (currently amended) The method of claim 19 wherein the identifying includes:

tracking an activity of users visiting the web site, and

identifying the group of [[real]] non-malicious users based at least in part on the tracked activity.

22. (previously presented) The method of claim 21 wherein the tracking includes determining, for each user, at least one of whether the user loads images, an age

of a cookie associated with each user, whether the user has javascript turned on, a type of browser used by the user, or an interval at which the user visits the web site.

23. (original) The method of claim 19 further comprising:

taking remedial measures in response to determining that the item has been click spammed.

24. (currently amended) The method of claim 19 wherein the determining a click rate of the item for the group of [[real]] non-malicious users includes:

estimating a percentage of [[real]] non-malicious users visiting the web site, and

setting a percentage of clicks of the item from [[real]] non-malicious users to approximately equal the estimated percentage.

25. (currently amended) The method of claim 24 wherein the determining whether the item has been click spammed includes:

determining whether an actual click rate of the item for the group of [[real]] non-malicious users differs from the set ~~click rate~~ percentage of clicks of the item.

26. (currently amended) The method of claim 19 wherein the determining a click rate of the item includes:

determining different click rates of the item for the group of [[real]] non-malicious users, the different click rates corresponding to different time periods.

27. (original) The method of claim 26 wherein the different time periods include different times of a day or week.

28. (original) The method of claim 26 wherein the different time periods include different months of a year.

29. (currently amended) A computer-readable memory device containing instructions for controlling at least one processor to perform a method for detecting a spamming of an advertisement displayed by a server, the method comprising:

identifying ~~real users visiting~~ non-malicious visitors to the server;

determining a click rate of the advertisement for the ~~real users~~ non-malicious visitors; and

determining whether the advertisement has been spammed based at least in part on the determined click rate for the ~~real users~~ non-malicious visitors.

30. (currently amended) A server comprising:

a memory configured to store at least one item; and

a processor configured to:

cause the at least one item to be displayed,

identify a number of ~~normal~~ non-malicious users accessing the server,

compare the number of ~~normal~~ non-malicious users to a total number of users to obtain a percentage,

set a click rate of the at least one item based at least in part on the percentage, and

determine whether the at least one item has been spammed based at least in part on the click rate.

31. (currently amended) A method comprising:

tracking activities of users visiting [[the]] a web site, the tracking including determining, for each user, at least one of whether the user loads images, an age of a cookie associated with each user, whether the user has javascript turned on, a type of browser used by the user, or an interval at which the user visits the web site; and

identifying [[real]] non-malicious users from among the users visiting the web site based at least in part on the tracked activities.

32. (new) The system of claim 16 where the means for identifying non-malicious visitors includes at least one of:

means for determining whether visitors to the web site load images,

means for determining whether the visitors to the web site have javascript turned on,

means for determining a type of browser used by the visitors to the web site,

means for determining an interval at which the visitors to the web site visit the web site, or

means for determining a type of items for which searches are performed by the visitors to the web site.

33. (new) The system of claim 16 where the means for tracking at least one activity of the identified non-malicious visitors includes at least one of:

means for determining a percentage of visitors in a group of visitors visiting the web site in a time period that are non-malicious visitors, and

where the means for determining an occurrence of click spamming includes:

means for estimating a percentage of non-malicious visitors selecting an advertisement associated with the web site during the time period to be approximately the percentage of non-malicious visitors visiting the web site during the time period, and

means for determining that the advertisement has been spammed when an actual percentage of non-malicious visitors selecting the advertisement during the time period is lower than the estimated percentage of non-malicious visitors selecting the advertisement during the time period.

34. (new) The computer-readable memory device of claim 17 where the determining whether the advertisement has been click spammed based at least in part on the determined percentage includes:

comparing the determined percentage of the non-malicious users clicking the advertisement to a percentage of non-malicious users clicking the advertisement from a different time period.

35. (new) The computer-readable memory device of claim 17 where the determining whether the advertisement has been click spammed includes:

estimating a percentage of non-malicious users clicking the advertisement to be approximately a percentage of non-malicious users accessing the server, and

determining that the advertisement has been clicked spammed when the determined percentage of non-malicious users clicking the advertisement is lower than the estimated percentage of non-malicious users clicking the advertisement.

36. (new) The server of claim 18 where, when determining whether the at least one advertisement has been click spammed, the processor is configured to:

compare the determined percentage of the non-malicious users clicking the at least one advertisement to a percentage of non-malicious users clicking the at least one advertisement from a different time period.

37. (new) The server of claim 18 where, when determining whether the at least one advertisement has been click spammed, the processor is configured to:

estimate a percentage of non-malicious users clicking the at least one advertisement to be approximately a percentage of non-malicious users visiting the server, and

determining that the at least one advertisement has been clicked spammed when the determined percentage of non-malicious users clicking the at least one advertisement is lower than the estimated percentage of non-malicious users clicking the at least one advertisement.

38. (new) The computer-readable memory device of claim 29 where the method further comprises:

determining a total number of visitors to the server, and

where the determining whether the advertisement has been spammed includes:

comparing the determined click rate for the non-malicious visitors to a click rate for the total number of visitors to the web site, and

determining that the advertisement has been spammed when the click rate for the total number of visitors exceeds the determined click rate for the non-malicious visitors.

39. (new) The computer-readable memory device 29 where the identifying non-malicious visitors to the server includes:

tracking a factor associated with visitors to the server, the factor including at least one of whether the visitors load images, ages of cookies associated with the visitors, whether the visitors have javascript turned on, types of browsers used by the visitors, or intervals at which the visitors visit the server, and

using the tracked factor to identify the non-malicious visitors to the server.

40. (new) The server of claim 30 where, when identifying a number of non-malicious users accessing the server, the processor is configured to:

track a factor associated with users accessing the server, the factor including at least one of whether the users load images, ages of cookies associated with the users, whether the users have javascript turned on, types of browsers used by the users, or intervals at which the users access the server, and

use the factor to identify the number of non-malicious users accessing the server.

41. (new) The server of claim 30 where the at least one item includes an advertisement.

42. (new) The method of claim 31 further comprising:

determining a quantity of the identified non-malicious users that clicks an advertisement associated with the web site; and

determining whether the advertisement has been spammed based on the determined quantity of the identified non-malicious users that clicks the advertisement.

43. (new) The method of claim 31 further comprising:

determining that spamming occurs on the web site based on a behavior of the non-malicious users visiting the web site.